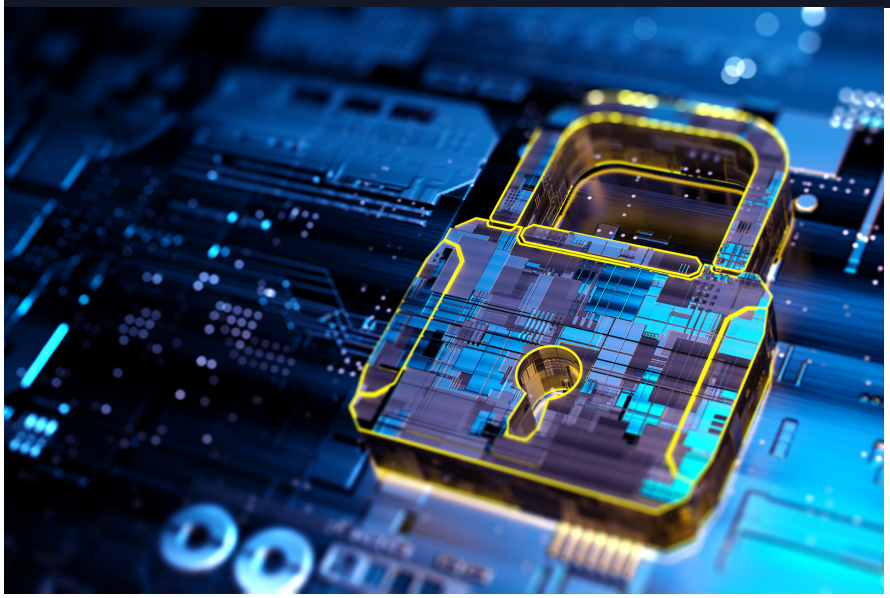
BARNES & THORNBURG LLP



ALERTS

COVID-19 Impacts And Increased Cybersecurity Risks

March 19, 2020

As the business world adjusts to dynamic changes in work environments brought about by the COVID-19 pandemic, businesses' data privacy and cyber security preparedness will be stress-tested like never before as employees work at home en masse.

Without formal data handling practices in place, employees working from home may not fully grasp that their actions could place sensitive information – that they and their employers are responsible for protecting – at risk. The potential exposure of sensitive information could include employee's personal information, which subsequently, can trigger state or federal data breach notification laws. Such exposures could result in significant legal liabilities to employers and issues for affected individuals like identity theft.

Employees working from home can create increased risks to data security, including, among others: 1) physical security of company devices, 2) the use of unsecured Wi-Fi networks, 3) increased phishing attempts and scams targeting remote workers, and 4) use of personal devices.

Physical Security of Company Devices

As many employers are requiring or permitting employees to work remotely, the physical security of company devices should be taken into consideration It is imperative to ensure company devices are password protected and that the information is encrypted, where possible, before relocating it from the usual workplace device to a remote device.

Not only do employers open themselves up to the risk of loss or theft of

RELATED PEOPLE

Brian J. McGinnis
Partner
Indianapolis

P 317-231-6437
F 317-231-7433
brian.mcginnis@btlaw.com

RELATED PRACTICE AREAS

COVID-19 Resources
Data Security and Privacy

company devices but, if applicable, unauthorized access to printed copies of sensitive documents. It is therefore essential for employers to reduce the risk of malicious actors gaining access to such sensitive information by imposing increased security measures for electronic data, as well as printed copies of documents and files.

Use of Unsecure Wi-Fi Networks

Unsecure Wi-Fi networks pose a risk to those working remotely because such networks allow malicious parties to spy on the network's internet traffic and, potentially intercept the information transferred through such networks.

Employers should ensure that their employees are aware of the risks involved and, if employees are permitted to use Wi-Fi networks, that such networks are protected with a strong password. Employers should also enable the remote workforce to use a company-provided virtual privacy network (VPN) to encrypt and secure online communications to protect sensitive information further.

Use of Personal Devices

Some companies may not have the ability to provide employees with a company laptop to take home. As a result, employees may be forced to conduct work tasks on their personal computers while at home. These personal devices may lack the physical and cybersecurity measures that companies typically use on company devices. Without these measures, employers faced an increased risk of someone gaining access to the less-secure personal computer and any work information held on that device.

Accordingly, employers should caution their employees to use devices that are equipped with the employer-provided security software and the latest manufacturer patches installed prior to permitting access to any remote system.

Increased Phishing Attempts and Scams Targeting Remote Workers

With more people working from home, malicious actors may take advantage of this drastic change in doing business by increasing phishing attacks, either by email or through a messaging app. Some of these may refer to the COVID-19 pandemic directly. These malicious actors may attempt to disguise their attacks in a way that relates to working from home. For instance, the World Health Organization (WHO) warns that "criminals are disguising themselves as WHO to steal money or sensitive information."

It is imperative that employers warn their employees that if they receive a communication that appears to be from WHO or any other governmental, charitable or a third-party institution, those employees should verify the address or contact their own internal IT security team.

- To avoid risk of suspicious emails or messages, people should look for the following:

- Does the email address match the person that it came from? When in doubt, reach out to the sender by phone to verify they sent the message.
- Does the tone of the message convey urgency? Is it asking you to respond quickly and without thinking?
- Does the message make sense? Does it sound like it came from the sender?
- Avoid clicking links that look suspicious.
- If typically provided, look for the [EXTERNAL] tag in the e-mail subject line.

To minimize risks, many companies already include warning banners on emails that originate outside of the company. Though with these new risks, employers should ensure that such banners continue to attach to email addresses from outside the company to further help employees parse out which COVID-19 updates are legitimate. An additional solution is to create a COVID-19 portal on the company website that employees can access for live company policy updates to ensure that an email communication from the company is legitimate.

Data Privacy Law Compliance – GDPR, CCPA and HIPAA

Working remotely may also implicate data privacy compliance in a new way for a business. Without a formal office setting, employees may become relaxed with their data protection practices. They may use their personal email to send work documents or conduct business on unsecured networks. As a result, personal information (PI) and personal health information (PHI) may is at risk of being obtained by an outside party.

It is important to specify a clear policy for remote-working employees to remind them of safe data practices. These policies may include:

- Specify in writing what employees can and cannot do in the handling of sensitive information
- Ask employees to specify which devices they will use for work and provide encryption services with a company certified security software
- Ask employees to password protect their personal networks with WPA2 encryption
- Identify and specify particular information and documents that require the utmost care in its handling
- Require any PI and PHI be encrypted before being transmittef
- Place limits on employees' access to various types of information until they are authorized
- Provide a VPN to connect to a company network

To protect its employees from COVID-19 and help "flatten the curve" via

social distancing, many businesses have chosen to send employees home to reduce the spread of the novel coronavirus. The unprecedented closing of business premises has prompted the urgency for businesses to ensure the safe handling and protection of personal information. Educating employees on best handling practices outside of the workplace is necessary to maintain the confidentiality and security of sensitive data.

For more information, contact the Barnes & Thornburg attorney with whom you work or Brian McGinnis at 317-231-6437 or brian.mcginnis@btlaw.com, Michael Baumert at 312-214-4570 or michael.baumert@btlaw.com, or Rocky Cislak at 317-229-3144 or rocky.cislak@blaw.com.